WHAT IS CLAIMED IS:

1. A method for controlling access to network, comprising the steps of:

establishing a trust relationship between a first supplicant and an authenticator both disposed on a wired network, wherein said first supplicant is authorized to access services on the network; and

extending said trust relationship to a second supplicant in communication with said first supplicant via a communication link, wherein said second supplicant is allowed access to said network services of the network.

2. The method of claim 1, wherein said authenticator is a switch, said first supplicant is an access point, and said second supplicant is a wireless client.

3. The method of claim 1, wherein said first supplicant in the step of establishing authenticates to an authentication server disposed on the network such that said trust relationship is established between said authenticator and said first supplicant.

4. The method of claim 3, wherein upon authentication of said first supplicant in the step of establishing, first supplicant information is stored in said authenticator that is a switch so that future communications with said switch from said first supplicant is authorized by said switch.

5. The method of claim 1, wherein said first supplicant authenticates to an authentication server disposed on the network such that said trust relationship is established between said authenticator and said first supplicant, said first supplicant and said authenticator authenticating mutually.

6. The method of claim 1, wherein once said trust relationship is established between said first supplicant and said authenticator, a message authentication check key is generated for signing subsequent communications between said first supplicant and said authenticator.

7. The method of claim 6, wherein said message authentication check key uniquely identifies said first supplicant to said authenticator.

8. The method of claim 1, wherein once said trust relationship is established between said second supplicant and said authenticator, a session key is generated for subsequent communications between said second supplicant and said first supplicant.

9. The method of claim 8, wherein said session key uniquely encrypts said communications via said communication link between said first and second supplicants.

10. The method of claim 1, wherein said communication link is an encrypted communication session between said first supplicant and said second supplicant created prior to said trusted relationship being extended to said second supplicant.

11. The method of claim 1, wherein said trust relationship is extended to said second supplicant in the step of extending by authenticating said second supplicant to an authentication server of the network.

12. The method of claim 1, wherein said trust relationship is extended to said second supplicant in the step of extending by storing second supplicant information in said authenticator whereafter packet traffic communicated between said second supplicant and said authenticator is transmitted through said first supplicant unimpeded.

13. The method of claim 1, wherein a handshake protocol is utilized between an authentication server of the network and said first supplicant.

14. The method of claim 1, wherein a handshake protocol is utilized between an authentication server of the network and said second supplicant.

15. The method of claim 1, wherein said second supplicant in the extending step is one of a laptop computer, handheld device, and electronic tablet each operable to communicate wirelessly to said first supplicant.

16. The method of claim 1, wherein said trust relationship between said first supplicant and said authenticator is invalidated by said authenticator until said first supplicant is properly authenticated to an authentication server, and said trust relationship between said second supplicant and said authenticator is invalidated by said authenticator until said second supplicant is properly authenticated to said authentication server.

17. The method of claim 1, wherein said authenticator is a switch that controls access to a switch port of said switch to which said first supplicant is connected, whereupon after successful authentication of said first supplicant and said second supplicant, said switch authorizes access to the network via said switch port.

18. The method of claim 1, wherein once said trust relationship is established in said first supplicant and said second supplicant, a MAC address of said first supplicant is stored in said authenticator and a MAC address of said second supplicant is stored in said authenticator.

19. The method of claim 1, wherein the network is an IEEE 802.1x architecture.

20. The method of claim 1, wherein the first supplicant, which is an access point, passes one or both of an access control list and quality-of-service parameters to the authenticator, which is a switch.

21. A method for controlling access to a network, comprising:

operatively disposing a switch on the network for providing access to network services of the network;

establishing a trust relationship between said switch and an access point disposed on the network in wired communication with said switch, said switch authorizing said access point to access to said network services via a switch port; and

extending said trust relationship to a client in communication with said access point via a communication link such that said trust relationship is extended to said client allowing said client access to said network services via said switch port.

22. The method of claim 21, wherein the network is an IEEE 802.1x architecture.

23. The method of claim 21, further comprising an authentication service accessible on the network by the switch such that authentication of a network entity is performed thereto.

24. The method of claim 23, wherein said authentication service is hosted on said switch such that said switch authenticates said access point.

25. The method of claim 23, further comprising an authentication server disposed on the network wherein said authentication server hosts said authentication service such that said trust relationship includes authenticating said access point to said authentication server via said switch.

26. The method of claim 21, further comprising an authentication server disposed on the network wherein said authentication server hosts an authentication service such that said trust relationship includes authenticating said access point to said authentication server via said switch, and then extending said trust relationship to said client by establishing said trust relationship to said client.

27. The method of claim 21, wherein said trust relationship includes mutually authenticating said access point via an authentication service disposed on the network.

28. The method of claim 21, wherein said trust relationship includes mutually authenticating said client via an authentication service disposed on the network

29. The method of claim 21, wherein said client communicates wirelessly to said access point.

30. The method of claim 21, wherein said client is in wired communication with said access point.

31. The method of claim 21, wherein said trust relationship of said access point includes mutual authentication between said access point and an authentication server disposed on the network, whereafter a unique message authentication check key is generated for maintaining secure communication between said access point and said switch.

32. The method of claim 21, wherein said trust relationship extended to said client includes mutual authentication between said client and an authentication server disposed on the network, whereafter a unique session key is generated by said authentication server and passed to said access point for maintaining secure communication between said access point and said client.

33. The method of claim 21, wherein when said trust relationship is established in said access point, a MAC address of said access point is stored in said switch to allow subsequent traffic of said access point unimpeded through said switch port, and when said trust relationship is established in said client, a MAC address of said client is stored in said switch to allow subsequent traffic of said client unimpeded through said switch port.

34. A method of providing access to an IEEE 802.1x network, comprising the steps of:

creating a trust relationship between a switch of the network and an access point of the network such that said access point accesses the network, said trust relationship created by,

authenticating said access point to an authentication server on the network to obtain access point authorization information; and

storing said access point authorization information in said switch such that subsequent communication between said switch and said access point is authorized;

establishing a communication link between said access point and a wireless client; and

extending said trust relationship to said wireless client such that said wireless client accesses the network, said trust relationship created by,

authenticating said wireless client to said authentication server on the network to obtain wireless client authorization information; and

storing said wireless client authorization information in said switch such that subsequent communication between said switch and said wireless client is authorized.

35. The method of claim 34, wherein said subsequent communication in the step of storing said wireless client authorization information provides packet traffic between said wireless client and said switch that is transmitted through said access point unaltered and unimpeded.

36. The method of claim 34, wherein a shared secret is established between said switch and said access point in the step of creating, and a session key is established between said access point and said wireless client in the step of extending.

37. The method of claim 34, wherein a handshake protocol is utilized between said authentication server and said access point in the step of authenticating said wireless client.

38. A system for providing access to network, comprising:

a first supplicant and an authenticator both disposed on a wired network in a trust relationship wherein said first supplicant is authorized to access services on the network; and

a second supplicant communicating with said first supplicant via a communication link such that said trust relationship is extended to said second supplicant allowing said second supplicant to access the network.

39. The system of claim 38, wherein said authenticator is a switch, said first supplicant is an access point, and said second supplicant is a wireless client.

40. The system of claim 38, wherein said first supplicant is authenticated to an authentication server disposed on the network such that said trust relationship is established between said authenticator and said first supplicant.

41. The system of claim 40, wherein upon proper authentication of said first supplicant, first supplicant information is stored in said authenticator that is a switch so that future communications with said switch from said first supplicant is authorized by said switch.

42. The system of claim 38, wherein said first supplicant is authenticated to an authentication server disposed on the network such that said trust relationship is established between said authenticator and said first supplicant, said first supplicant and said authentication authenticating mutually.

43. The system of claim 38, wherein once said trust relationship is established between said first supplicant and said authenticator, a message authentication check key is generated for subsequent communications between said first supplicant and said authenticator.

44. The system of claim 43, wherein said message authentication check key uniquely identifies said first supplicant to said authenticator.

45. The system of claim 38, wherein once said trust relationship is established between said second supplicant and said authenticator, a session key is generated for subsequent communications between said second supplicant and said first supplicant.

46. The system of claim 45, wherein said session key uniquely encrypts said communication link between said first and second supplicants.

47. The system of claim 38, wherein said communication link is an encrypted communication session between said first supplicant and said second supplicant created prior to said trusted relationship being extended to said second supplicant.

48. The system of claim 38, wherein said trust relationship is extended to said second supplicant by authenticating said second supplicant to an authentication server of the network.

49. The system of claim 38, wherein said trust relationship is extended to said second supplicant by storing second supplicant information in said authenticator whereafter packet traffic communicated between said second supplicant and said authenticator is transmitted through said first supplicant unimpeded.

50. The system of claim 38, wherein a handshake protocol is utilized between an authentication server of the network and said first supplicant.

51. The system of claim 38, wherein a handshake protocol is utilized between an authentication server of the network and said second supplicant.

52. The system of claim 38, wherein said second supplicant is one of a laptop computer, handheld device, and electronic tablet each operable to communicate wirelessly to said first supplicant.

53. The system of claim 38, wherein said trust relationship is invalidated by said authenticator until said first supplicant is properly authenticated to an authentication server, and said trust relationship is invalidated by said authenticator until said second supplicant is properly authenticated to said authentication server.

54. The system of claim 38, wherein said authenticator is a switch that controls access to a switch port of said switch to which said first supplicant is connected, whereupon successful authentication of said first supplicant and said second supplicant, said switch authorizes access to the network via said switch port.

55. The system of claim 38, wherein once said trust relationship is established in said first supplicant and said second supplicant, a MAC address of said first supplicant is stored in said authenticator and a MAC address of said second supplicant is stored in said authenticator.

56. The system of claim 38, wherein the network is an IEEE 802.1x architecture.

57. The system of claim 38, wherein the first supplicant, which is an access point, passes one or both of an access control list and quality-of-service parameters to the authenticator.

58. A system for controlling access to a network, comprising:

a switch operatively disposed on the network for providing access to network services of the network;

an access point disposed on the network in wired communication with a switch port of said switch, said access point in a trust relationship wherein said switch authorizes said access point to access to said network services via said switch port; and

a client in communication with said access point via a communication link such that said trust relationship is extended to said client allowing said client access to said network services via said switch port.

59. The system of claim 58, wherein the network is an IEEE 802.1x architecture.

60. The system of claim 58, further comprising an authentication service accessible on the network such that authentication of a network entity is performed thereto.

61. The system of claim 59, wherein said authentication service is hosted on said switch such that said switch authenticates said access point.

62. The system of claim 59, further comprising an authentication server disposed on the network wherein said authentication server hosts said authentication service such that said trust relationship includes authenticating said access point to said authentication server via said switch.

63. The system of claim 58, further comprising an authentication server disposed on the network wherein said authentication server hosts an authentication service such that said trust relationship includes authenticating said access point to said authentication server via said switch, and then extending said trust relationship to said client by establishing said trust relationship to said client.

64. The system of claim 58, wherein said trust relationship includes mutually authenticating said access point via an authentication service disposed on the network.

65. The system of claim 58, wherein said trust relationship includes mutually authenticating said client via an authentication service disposed on the network

66. The system of claim 58, wherein said client communicates wirelessly to said access point.

67. The system of claim 58, wherein said client is in wired communication with said access point.

68. The system of claim 58, wherein said trust relationship of said access point includes mutual authentication between said access point and an authentication server disposed on the network, whereafter a unique message authentication check key is generated for maintaining secure communication between said access point and said switch.

69. The system of claim 58, wherein said trust relationship extended to said client includes mutual authentication between said client and an authentication server disposed on the network, whereafter a unique session key is generated by said authentication server and passed to said access point for maintaining secure communication between said access point and said client.

70. The system of claim 58, wherein when said trust relationship is established in said access point, a MAC address of said access point is stored in said switch to allow subsequent traffic of said access point unimpeded through said switch port, and when said trust relationship is established in said client, a MAC address of said client is stored in said switch to allow subsequent traffic of said client unimpeded through said switch port.